Computer and Cyber Ethics

Dr. Bhaskar Mondal

Learning Objectives

Describe what the term *information systems ethics* means.

Explain what a code of ethics is and describe the advantages and disadvantages.

Define the term *intellectual property* and explain the protections provided by copyright, patent, and trademark.

Describe the challenge that information technology brings to individual privacy.

Computer and Internet Crime

Quote: In view of all the deadly computer viruses that have been spreading lately, Weekend Update would like to remind you: when you link up to another computer, you're linking up to every computer that that computer has ever linked up to. (Dennis Miller, Saturday Night Live)

It's not gold or oil - the most valuable commodity today is information.

The Economist

Subscribe

Regulating the internet giants

The world's most valuable resource is no longer oil, but data

data economy demands a new approach to antitrust rules

On the Internet

INFORMATION CAN BE CREATED,

STORED,

ACCESSED AND

RETRIEVED DATA

Privacy

- Privacy is a state where an individual can work on his/her information in seclusion,
- with an objective of revealing their identity or information only to selected individuals.
- Privacy also means to stay in a state of anonymity.

Real Case: Sasser Worm

- Unleashed in April 2004, the Sasser worm hit IT systems around the world hard and fast.

  http://www.symantec.com/security_response/writeup.jsp?docid=2004-050116-1831-99

  http://www.pcworld.com/article/id,115979-page,1/article.html
- Didn't spread through e-mail, but moved undetected across the Internet from computer to computer
- Exploited the weakness in Windows XP and 2000
- By the first week of May, American Express, the Associated Press, the British Coast Guard, universities and hospitals reported that Sasser worm has swamped their systems
- Delta Airlines cancelled around 40 flights and delayed many others

Sasser Worm

- Microsoft posted a $250,000 reward
- By mid-May, authorities apprehended Sven Jaschan, a German teenager.
- Jaschan confessed and was convicted after a three-day trial:

  http://news.bbc.co.uk/2/hi/europe/3695857.stm
- He could receive up to five years in prison, but because he was tried as a minor, the court suspended his 21-month sentence, leaving him with only 30 hours of community service:

  http://news.bbc.co.uk/2/hi/technology/4659329.stm

Sasser Worm

- Just a few month after Jaschan's indictment, the Securepoint, a German IT security company hired him as a programmer:

  http://www.sophos.com/pressoffice/news/articles/2004/09/va_jaschanjob.html
- Lawyers disagree over punishment in Sasser trial:

  http://www.computerworld.com/securitytopics/security/story/0,10801,103005,00.html?source=x73

Introduction to Ethics

Quote from Aristotle:

"Man, when perfected, is the best of the animals, but when separated from law and justice, he is the worst of all"

What is Ethics?

- Each society forms a **set of rules** that establishes the boundaries of generally accepted behavior.
- These rules are often expressed in statements about how people should behave, and they fit together to form the **moral code** by which a society lives.
- **Ethics** is the set of beliefs about right and wrong behavior.
- Ethical behavior conforms to generally accepted social norms, many of which are almost universal.
- **Virtues** are habits that incline people to do what is acceptable, and **vices** are habits of unacceptable behavior
- People's virtues and vices help define their **value system** – the complex scheme of moral values by which they live

Morality and Ethics

- *Principles concerning the distinction between right and wrong or good and bad behavior*
- *Moral principles that govern a person's behavior or the conducting of an activity*
- In general parlance, morality as a personal set of values on what is “good" and “bad", whereas ethics tend to be concerned with an external body denning what is “right" and “wrong".

Computer Ethics

- Ethics are a set of moral principles that governs an individual or a group on what is acceptable behavior while using a computer.

Information Systems Ethics

- Ethics
  - Set of moral principles.
  - Principles of conduct that guide an individual or group.
- New Technology
  - Creates new uses in society
  - Creates environments and situations that people haven’t seen before.

Objectives of ethics

Justice/equity

Freedom

Care and compassion

Participation

Sharing

Sustainability

Responsibility

What is the Unethical behavior

DIGITAL PLAGIARISM

BREAKING COPYRIGHT AND SOFTWARE THEFT

IMPROPER USE OF COMPUTER RESOURCES

Technology & Ethics

Henry Ford's Assembly Line

- Created advantage in that cars could be manufactured more quickly.
- De-valued human work/skill in the production process.

Volkswagen Diesel Deception

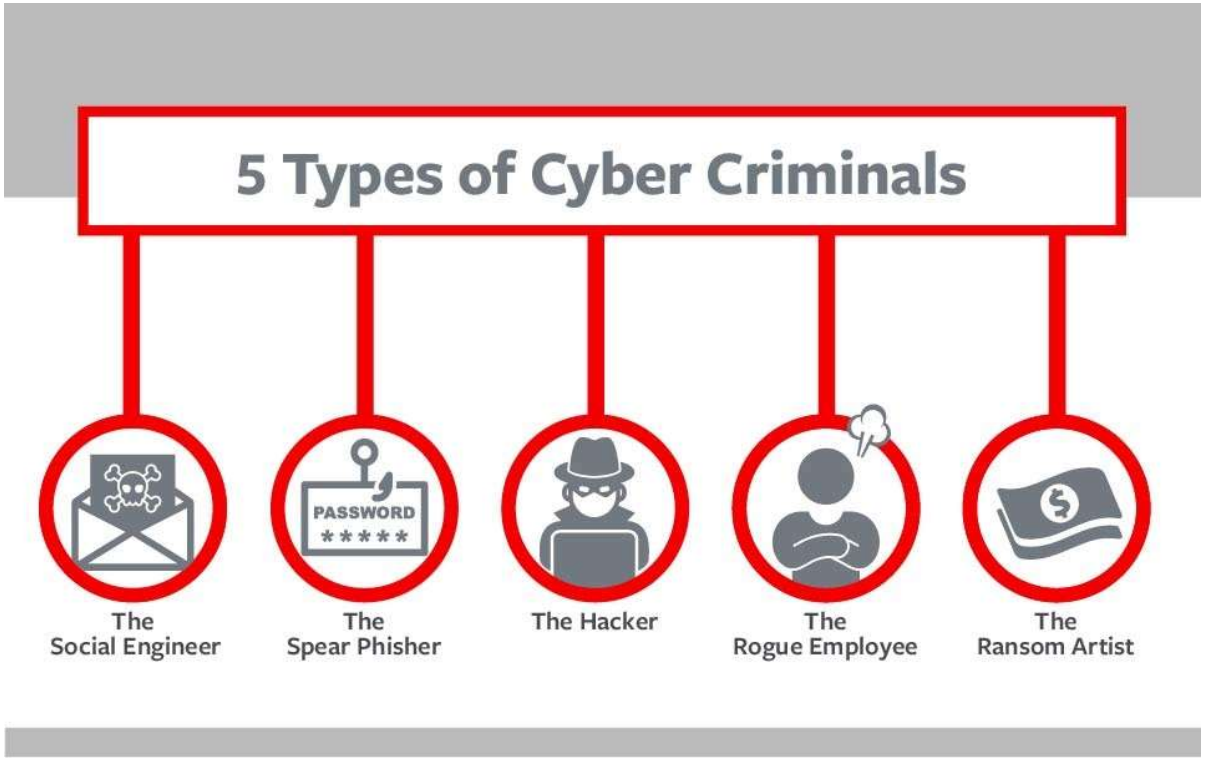
- Sensors in cars for testing and software programming allowed VW to cheat on emissions testing.

Code of Ethics

- Documented set of acceptable behaviors for professional or social groups.
- Defined by the group.
- Identifies specific actions as appropriate or inappropriate.
- Sample Codes
  - American Marketing Association
  - Academy of Management

Cyber Crime

- Identity Thrift
- Click Fraud
- Hacking
- Copyright infringement



Ethical rules for the computer users

- One shall not use a computer to harm other people.
- One shall not interfere with others' computer work.
- One shall not snoop around in other 's computer les. Respect the privacy of others, just as you expect the same from others.
- Do not use computers to steal others' information.
- One shall not use a computer to bear false witness.

Ethical rules for the computer users

- One shall not copy or use proprietary software for which one have not paid.
- One shall not use others' computer resources without authorization or proper compensation. Do not access les without the permission of the owner.
- One shall not appropriate others' intellectual output.
- One shall think about the social consequences of the program written or of the system designed by one.
- One shall always use a computer in ways that insure consideration and respect for one's fellow humans.

Ethical rules for the computer users

- Do not copy copyrighted software without the author's permission. Always respect copyright laws and policies.
- Use Internet ethically.
- Complain about illegal communication and activities, if found, to Internet service Providers and local law enforcement authorities.
- Users are responsible for safeguarding their User Id and Passwords. They should not write them on paper or anywhere else for remembrance.
- Users should not intentionally use the computers to retrieve or modify the information of others, which may include password information, les, etc.

Examples of Specific Admonitions

- “No one should enter or use another’s computer system, software, or data files without permission.”
- “Designing or implementing systems that deliberately or inadvertently demean individuals or groups is ethically unacceptable.
- “Organizational leaders are responsible for ensuring that computer systems
  enhance, not degrade, the quality
  of working life.”

Ethics and the Internet

- Acceptance
- Sensitivity to National and Local cultures
- While using e-Mail and chatting
- Pretending someone else
- Avoid Bad language
- Hide personal information
- Downloading (Creative Commons)
- Supervision
- Encourage children to use Internet
- Access to Internet

Professional Codes of Ethics

- A professional code of ethics states the principles and core values that are essential to the work of a particular occupational group.
- Association of Computing Machinery ACM (founded 1947) has a code of ethics and professional conduct. See: http://www.acm.org/constitution/code.html
- Association of Information Technology Professionals AITP (founded 1996) – provides quality IT-related education, information on relevant IT issues, and forums for networking with experienced peers and other IT professionals. The AITP also has a code of ethics, see:

  http://www.aitp.org/join/SCOH17CodeEthicsStdsCdt.pdf

Professional Codes of Ethics

- Computer Society of the Institute of Electrical and Electronics Engineers (IEEE – CS) (founded in 1946). The Software Engineering Code of Ethics and Professional Practice: http://www.acm.org/serving/se/code.htm

- Project Management Institute (PMI) – established in 1969. PMI Member Code of Ethics: http://www.pmi.org/info/AP_MemEthStandards.pdf

Association for Computing Machinery (ACM) Code of Ethics

- 24 imperatives of personal responsibility.
  - Contains issues that professionals will have to deal with.
  - Section 1: General Moral Imperatives (ex. Avoid harm to others.)
  - Section 2: Professional Conduct (ex. Maintain professional competence.)
  - Section 3: Individuals with Leadership
    - Roles (ex. Create opportunities for people.)
  - Section 4: Compliance with the
    - Ethical Code (ex. Promote ethics.)

Acceptable Use Policies (AUP)

- Guidelines for behavior when using technology services.
- Virginia Tech AUP
- CPP AUP
  - “Individuals may not access, copy, add, alter, damage, delete or destroy any data or computer software on any other computer unless specifically authorized.”
  - “The student shall be held accountable for his/her own behavior and for the inappropriate activity originating from his/her unit or computer. All passwords should be secure.”

Common Ethical Issues for IT Users

- **Software Piracy**: a common violation occurs when employees copy software from their work computers for use at home
- **Inappropriate Use of Computing Resources**: some employees use their work computers to surf popular Web sites that have nothing to do with their jobs.

  "Half of Fortune 500 companies have dealt with at least one incident related to computer porn in the workplace over the past 12 months, according to a survey released.
  Corporations are taking the problem seriously and fired the offenders in 44% of the cases and disciplined those responsible in 41% of the instances".

  (China Martens, Survey: Computer porn remains issue at U.S. companies, Computer-world, June 21, 2005

  http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=102664

Common Ethical Issues for IT Users

- **Inappropriate Sharing of Information:**
  - Organizations stored vast amount of information that can be classified as private or confidential.
  - Private data describes individual employees – for example, salary, attendance, performance rating, health record.
  - Confidential information describes a company and its operations: sales, promotion plans, research and development.
  - Sharing this information with unauthorized party, even inadvertently, has violated someone's privacy or created the potential that company information could fall into the hands of competitors.

Supporting The Ethical Practices of IT Users

- **Defining and Limiting the Appropriate Use of IT Resources**
  - Companies must develop, communicate and enforce written guidelines that encourage employees to respect corporate IT resources and use them to enhance their job performance.
  - Effective guidelines allow some level of personal use while prohibiting employees from visiting objectionable Web sites or using company e-mail to send offensive or harassing messages.

Supporting The Ethical Practices of IT Users

- **Establishing Guidelines for Use of Company Software**
  - Company IT managers must provide clear rules that govern the use of home computers and associated software.
  - The goal should be to ensure that employees have legal copies of all software
- **Structuring Information Systems to Protect Data and Information**
  - Implement system and procedures that limit data access to employees who need it.
  - Employees should be prohibited from accessing the data about research and development results, product formulae, and staffing projections if they don't need it to do their job

Supporting The Ethical Practices of IT Users

- **Installing and Maintaining a Corporate Firewall**
  - Firewall is a software or hardware device that serves as a barrier between a company and the outside world and limits access to the company's network based on the Internet usage policy.
  - Firewall can be configured to serve as an effective detergent unauthorized Web surfing by blocking access to specific, objectionable Web sites.
  - Firewall can serve as an effective barrier to incoming e-mail from certain Web sites, companies or users
  - Can be programmed to block e-mail with certain kinds of attachments, which reduces the risk of harmful computer viruses

Computer and Internet Crime
IT Security Incidents

- The security of IT used in business is very important
- Although, the necessity of security is obvious, it often must be balanced against other business needs and issues
- IT professionals and IT users all face a number of ethical decisions regarding IT security:

Ethical Decisions Regarding IT Security

- Business managers, IP professionals, and IT users all face a number of ethical decisions regarding IT security:
  - If their firm is a victim of a computer crime, should they pursue prosecution of the criminals at all costs, should they maintain a low profile to avoid the negative publicity, must they inform their affected customers, or should they take some other actions?
  - How much effort and money should be spent to safeguard against computer crime (how safe is safe enough?)

Ethical Decisions Regarding IT Security

- If their firm produces software with defects that allow hackers to attack customer data and computers, what actions should they take?
- What tactics should management ask employees to use to gather competitive intelligence without doing anything illegal?
- What should be done if recommended computer security safeguards make life more difficult for customers and employees, resulting in lost sales and increasing costs?

What could be done to deal with the increasing number of IT-related security incidents, not only in USA but around the world?

- To deal with the incidents, the Computer Emergency Response Team Coordination Center (CERT/CC) was established in 1988 at the Software Engineering Institute (SEI) – federally funded research and development center at Carnegie Mellon:
  - Study Internet Security vulnerabilities
  - Handle Computer Security Incidents
  - Publish Security Alerts
  - Research long-term changes in networked systems
  - Develop information and training
  - Conduct ongoing public awareness campaign
- FBI Cyber Program, Internet Crime Complaint Center

  http://www.fbi.gov/cyberinvest/cyberhome.htm

Some Statistics

- The number of security problems reported to CERT/CC grew between 1997 and 2003 from 2134 to 137,529
- From 2004 the CERT/CC no longer publishes the number of incidents reported

Advantage of Ethical Codes

- Adds clarity to the understanding of acceptable standards of behavior.
- Communicates common guidelines for everyone to follow.
- What happens if you don’t follow the organizations ethical code?
  - ACM – voluntary
  - State Bar Association – revoke license

Disadvantage of Ethical Codes

- May not reflect the ethical of every member of the group.
- Many times, it isn't enforceable. It's a code of conduct, not a legal document.

Challenges

- Increasing complexity increases vulnerability:
  - The computing environment has become very complex
  - Networks, computers, OS, applications, Web sites, switches, routers and gateways are interconnected and driven by hundreds of millions of lines of code
  - The number of possible entry points to a network expands continually as more devices are added, increasing the possibility of security breaches

Challenges

- Higher computer user expectations:
  - Time means money
  - Help desks are under intense pressure to provide fast responses to user's questions.
  - Sometimes forgets to verify user's identities, or to check authorization to perform a requested action

Challenges

- Expanding and changing systems introduce new risks:
  - Businesses had moved from an era of stand-alone computers to a network era – personal computers connect to networks with millions of other computers all capable of sharing information.
  - E-commerce, mobile computing, collaborative work groups, global business
  - It is increasingly difficult to keep up with the pace of technological change, successfully perform an ongoing assessment of new security risks, and implement approaches for dealing with them

Challenges

- Increases reliance on commercial software with known vulnerabilities:
  - **Exploit** is an attack on an information system that takes advantage of a particular system vulnerability. Often, this attack is due to poor system design or implementation.
  - Once a vulnerability is discovered, software developers create and issue a "fix" or **patch** to eliminate the problem. Users are responsible for obtaining and installing the patch. Any delay in installing a patch exposes the user to a security breach.
  - A rate of discovering software vulnerabilities exceeds 10 per day, creating a serious work overload for developers who are responsible for security fixes.

Challenges: Increases reliance on commercial software with known vulnerabilities:

- **A zero-day** attack take place BEFORE the security community, or a software developer knows about a vulnerability or has been able to repair it.

  http://www.computerworld.com/securitytopics/security/hacking/story/0,10801,90447,00.html?f=x583
- Malicious hackers are getting better and faster at exploiting flaws.
- The SQL Slammer worm appeared in January 2004, eight month after the vulnerability it targeted was disclosed:

  http://www.computerworld.com/softwaretopics/software/groupware/story/0,10801,89637,00.html

Challenges: Increases reliance on commercial software with known vulnerabilities:

- In August 2005, the ZOTOB computer worm began targeting corporate networks that run Windows 2000, less than a week after Microsoft released a critical patch addressing the vulnerability

  http://www.cnn.com/2005/TECH/internet/08/16/computer.worm/index.html

- In an attempt to avoid further attacks and the ultimate zero-day attack, computer security firms and software manufactures are paying hackers to identify vulnerabilities before they can be exploited.

  http://www.businessweek.com/magazine/content/05_34/b3948022_mz011.htm?chan=tc